5 de junho de 2017

Ao Senhor Deputado
Orlando Silva
Câmara dos Deputados, anexo 4, gabinete 923
Praça dos Três Poderes
Brasília, DF CEP 70165-900

Assunto: Comentários da BSA sobre o PL 5276/2016 – Dados Pessoais

A BSA| The Software Alliance[1] agradece a oportunidade de participar da importante discussão sobre o futuro da proteção de dados no Brasil. Um regime regulatório balanceado que proteja a privacidade dos consumidores sem comprometer a inovação e o potencial da economia digital trará muitos benfícios ao país.

Como uma organização global, a BSA acompanha ativamente o desenvolvimento de políticas públicas na área de privacidade de dados em todo o mundo. Os membros da BSA têm um comprometimento profundo e duradouro com a proteção de dados pessoais de consumidores em diferentes tecnologias e modelos de negócios pois reconhecem que os consumidores só se sentem confortáveis em aproveitar os benefícios de novas tecnologias quando sabem que não perderão o controle sobre seus

---

[1] *BSA | The Software Alliance (www.bsa.org) é a principal representante global do setor de software perante governos e no mercado internacional. Seus membros incluem as empresas mais inovadores do mundo, que criam soluções de software que impulsionam a economia e melhoram a vida moderna. Sediada em Washington, DC, e com operações em mais de 60 países, a BSA é pioneira em programas de conformidade que promovem o uso de software legítimo e apóia políticas públicas que fomentam a inovação em tecnologia e fortalecem o crescimento da economia digital.*

Os membros da BSA incluem: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

dados pessoais. Nesse sentido, a BSA e seus membros parabenizam e apoiam o esforço do Congresso em criar um quadro jurídico abrangente e equilibrado para a proteção dos dados pessoais.

Com o objetivo de colaborar com a discussão do PL 5276/2016 que está sendo conduzida pela Comissão Especial, a BSA agradece a oportunidade de compartilhar seus pontos de vista sobe os seguintes tópicos para contribuir com o aprimoramento do projeto de lei:

- Escopo Territorial
- Definição de Dados Pessoais
- Consentimento
- Outras Bases Legítimas para o Tratamento de Dados
- Alocação de Responsabilidades e Obrigações
- Transferências Internacionais de Dados
- Segurança de Dados
- Início da Vigência da Lei

ESCOPO TERRITORIAL:

O uso difundido da Internet, os tecnologias de computação em nuvem, o crescimento da “Internet das Coisas” e a contínua expansão da economia movida por dados faz com que a aplicação do princípio da territorialidade fique mais complexa, já que pode ser praticamente impossível identificar a localização exata de uma atividade que acontece online e determinar que a mesma tenha ocorrido em um determinado país.

A BSA sugere que a Lei de Proteção de Dados Pessoais seja aplicável em referência a qualquer operação de tratamento realizada, por pessoa natural ou por pessoa jurídica de direito público ou privado, contanto que: 1) os dados pessoais de pessoas residentes no Brasil sejam especificamente o alvo da coleta, e; 2) os dados pessoais forem propositalmente coletados no território nacional e se refiram a pessoas residentes no Brasil no momento da coleta **e** que a coleta seja realizada por uma entidade estabelecida no Brasil ou sujeita às leis brasileiras em virtude de regras de direito internacional.

Modificações recomendadas [2]

Art. 3- *Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede ou do país onde estejam localizados os dados, desde que:*

I – A informação coletada refira-se especificamente a pessoas residentes no Brasil; e ~~a operação de tratamento seja realizada no território nacional~~

~~II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou~~

II~~I~~ – os dados pessoais objeto do tratamento sejam propositalmente coletados no território nacional; e

III – a referida coleta seja realizada por uma entidade estabelecida no Brasil ou sujeita à legislação brasileira em virtude do direito público internacional.

~~Parágrafo único. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.~~

DEFINIÇÃO DE DADOS PESSOAIS

Observamos que a aplicação de obrigações legais muito rigorosas a uma vasta gama de dados, independentemente do contexto e potencial de danos ao usuário, reduzirá a inovação orientada por dados no Brasil, com impacto negativo sobre o crescimento econômico do país.

Assim, sugerimos que a legislação brasileira adote um conceito de dados pessoais baseado no contexto, sob o qual os dados sejam considerados "dados pessoais" somente quando sejam referentes a uma pessoa natural identificada ou identificável.

---

[2] Ao longo deste documento, as referências taxadas (~~texto~~) indicam sugestões de exclusão de texto original do projeto e as referências sublinhadas (texto) indicam sugestões de adição ao texto original do projeto.

Modificações recomendadas

Art. 5º – Para os fins desta Lei, considera-se:

I. dado pessoal: dado relacionado à pessoa natural identificada ou identificável~~, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;~~
...

<u>CONSENTIMENTO</u>

Apesar de reconhecermos que o consentimento do titular é uma forma válida de legitimar o tratamento de dados pessoais, o mesmo não deve ser a única forma. Outras bases legais para o tratamento de dados devem ser consideradas igualmente válidas.

A exigência de consentimento como forma primária de legitimar o processamento é problemática, pois pode haver casos em que a obtenção do consentimento não seja adequada ou apropriada. Por exemplo, se uma instituição financeira precisar coletar informações sobre uma dívida pendente para autorizar procedimentos de cobrança, pode não ser adequado solicitar a autorização do titular dos dados para fazê-lo. Entretanto, existe um interesse comercial legítimo que justificaria a coleta de dados neste caso (vide seção abaixo para mais detalhes sobre interesse legítimo).

Modificações recomendadas

Aplaudimos as mudanças que já foram incorporadas ao projeto de lei reconhecendo outros meios de legitimar o tratamento de dados, incluindo o legítimo interesse. Essas mudanças devem ser mantidas. Em situações nas quais o consentimento for necessário, é importante que a legislação foque nos fins e não nos meios através dos quais o consentimento é fornecido. Contanto que o consentimento seja dado de forma livre, específica, informada e de maneira inequívoca, o mesmo deverá ser aceito.

<u>OUTRAS BASES LEGÍTIMAS PARA O TRATAMENTO DE DADOS</u>:

É importante que a legislação brasileira siga as melhores práticas internacionais que aceitam uma série de bases legais para o tratamento de dados além do consentimento.

O tratamento de dados com base no interesse legítimo do responsável deve ser autorizado porque permitirá que novos negócios baseados em análise de dados continuem beneficiando o Brasil. O interesse legítimo desempenha um papel particularmente importante quando não é adequado ou apropriado que o que o responsável pelo tratamento de dados obtenha o consentimento para legitimar a coleta e tratamento dos dados ou quando ainda é prematuro celebrar um contrato com um consumidor. Contanto que os direitos e liberdades fundamentais do titular sejam respeitados, o interesse legítimo deve ser aceito como base para o tratamento de dados.

Deve também ser permitido o tratamento de dados para garantir a segurança das redes e da informação ou para prevenir fraude. Permitir que os dados sejam tratados nestes casos é importante para que as empresas possam proteger as suas redes e os dados pessoais que lhes são confiados, impedindo o acesso não autorizado, a distribuição de códigos maliciosos e o bloqueio de prestação de serviços (ataques de negação de serviços).

Modificações recomendadas

Recomendamos que o inciso X seja inserido no artigo 7, como segue:

Art 7- *O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*

....

X – quando o tratamento é necessário para os propósitos de assegurar a segurança da informação e da rede ou prevenir fraudes.

Também recomendamos que o artigo 10 seja modificado conforme texto abaixo.

Art. 10º *- O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais quando razoavelmente necessário para apoiar ou promover a prestação de serviços que beneficiem o titular ou para aprimorar tais serviços, para a prática de atividades e funções do responsável, ou quando o consentimento for inviável ou desnecessário. ~~e baseado em uma situação concreta~~, respeitados os direitos e liberdades fundamentais do titular.*

§1º O legítimo interesse deverá contemplar as legítimas expectativas do titular quanto ao tratamento de seus dados, de acordo com o disposto no art. 6º, inciso II.

§2º O responsável deverá adotar medidas para garantir a transparênia do tratamento de dados baseado no seu legítimo interesse~~, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais~~.

§ 3º Quando o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento.

§ 4º O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo.

ALOCAÇÃO DE RESPONSABILIDADE E OBRIGAÇÕES

As relações entre o operador (processadores) e a pessoa responsável (controlador dos dados), bem como entre o outorgante e outorgado, devem ser regidas por contratos ou outros atos legalmente vinculantes, cuja violação sujeitaria as partes às disposições do Código Civil.

Essa clara alocação de responsabilidade e obrigação legal é crucial e garante que a prática crescente e difundida da terceirização não cause confusão no sistema. Essa atribuição permite que o titular dos dados e as autoridades saibam a quem recorrer caso ocorra um problema, e que as empresas tenham clareza sobre suas funções e responsabilidades.

A inserção de responsabilidade solidária sobre o operador/ ou o cessionário teria uma série de consequências indesejáveis e prejudicaria a relação entre a pessoa responsável e o operador, criando uma dificuldade injustificada. Além disso, isto impactaria negativamente investimentos potenciais em processamento de dados e terceirização de serviços que beneficiariam o Brasil.

As pessoas responsáveis devem ter a obrigação primária de assegurar o cumprimento da lei de privacidade aplicável, enquanto os operadores devem ser obrigados a cumprir as instruções da pessoa responsável e garantir a segurança dos dados que processam.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

Modificações recomendadas

Art. 34. A autorização referida no inciso IV do **caput** do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, ~~apresentadas em~~ por meio de cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, através de acordos para transferência de dados em conformidade com cláusulas contratuais padrão ou ~~em~~ normas corporativas globais ou que incluam estipulações que assegurem conformidade com esta Lei. ~~, nos termos do regulamento~~.

§ 1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular~~, garantida a responsabilidade solidária do cedente e do cessionário, independentemente de culpa~~.

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou do conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou do conglomerado sem necessidade de autorizaçãoes específicas, observados os princípios gerais de proteção e os direitos do titular.

§ 3º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

§ 4º As garantias suficientes de observância dos princípios gerais de proteção e dos direios do titular referidas no caput serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos § 1º e § 2º do art. 45.

Art. 35. *A pessoa responsável ~~O cedente e o cessionário~~ deve permanecer como a principal responsável ~~respondem solidária e objetivamente~~ pelo tratamento de dados e por fornecer reparação aos titulares. A responsabilidade deve ser alocada entre as pessoas responsáveis pelo tratamento de acordo com a sua culpa comprovada que dê ensejo ao dano. ~~independentemente do local onde estes se localizem, em qualquer hipótese~~.*

TRANSFERÊNCIAS INTERNACIONAIS:

A capacidade de transferir dados internacionalmente é a força vital da economia digital moderna. As organizações que transferem dados devem tomar medidas apropriadas para garantir que as informações do usuário sejam devidamente protegidas.

A abordagem "transferência proibida a menos que..." da legislação europeia tem sido bastante criticada porque conflita com o vasto aumento de fluxo de dados globais que ocorreu nos últimos 20 anos, desde sua adoção.

O modelo de responsabilização ("accountability model") estabelecido pela OCDE e subsequentemente endossado a integrado a diversos sistemas jurídicos e princípios de privacidade, incluindo as Regras de Privacidade Internacionais da Cooperação Econômica Ásia-Pacífico ("APEC CBPR") e a Lei de Proteção de Informações Pessoais do Canadá - que recebeu uma determinação de adequação da UE - ofereceria uma abordagem à governança internacional de dados que protegeria os titulares dos dados e fomentaria fluxos robustos e otimizados de dados.

Tal modelo de responsabilização, que exige que as organizações que coletam dados sejam responsáveis pela sua proteção não importando onde ou por quem os dados sejam processados, protegeria adequadamente os usuários. Esta abordagem requer que as organizações que transferem dados tomem as medidas apropriadas para garantir que quaisquer obrigações – estabelecidas em lei, diretrizes ou compromissos firmados em políticas de privacidade - sejam cumpridas.

Assim, recomendamos fortemente que o governo brasileiro considere os benefícios de permitir transferências internacionais com base em compromissos assumidos em acordos de cooperação internacional, incluindo códigos internacionais de conduta da indústria ou estruturas desenvolvidas por meio de processos abertos, com a participação dos interessados ("multistakeholder process").

Além disso, deve ser instituído um sistema de reconhecimento mútuo de cláusulas contratuais padrão e para padrões corporativos globais, a fim de evitar exigências globais múltiplas e potencialmente contraditórias.

Modificações recomendadas

Art. 33. *A transferência internacional de dados pessoais somente é permitida nos seguintes casos:*

I – para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;

II – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

III – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

IV – quando o órgão competente autorizar a transferência;

V - quando a transferência for resultado de ~~em~~ compromisso assumido em acordo de cooperação internacional, incluindo códigos de conduta internacionais do setor privado ou mecanismos desenvolvidos através de processos abertos, com participação dos interessados (“multistakholder process”);

VI – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24; ou

VII – quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.

Parágrafo único. O nível de proteção de dados do país estrangeiro será avaliado pelo órgão competente, que levará em conta:

I – as normas gerais e setoriais da legilsação em vigor no país de destino;

II – a natureza dos dados;

III- a observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

IV – a adoção de medidas de segurança previstas em regulamento; e

V – as outras circunstâncias específicas relativas à transferência.

Conforme acima colocado, o caput do 34 também deve ser alterado.

Art. 34. *A autorização referida no inciso IV do* ***caput*** *do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, ~~apresentadas em~~ por meio de cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, através de acordos para transferência de dados em conformidade com cláusulas contratuais padrão ou ~~em~~ normas corporativas globais ou que incluam estipulações que assegurem conformidade com esta Lei. ~~, nos termos do regulamento~~.*

....

SEGURANÇA E VIOLAÇÃO DE DADOS

A BSA apoia a criação de um sistema de notificação de violação de dados aplicável a todos os negócios e organizações. Tal exigência poderia incentivar entidades a garantir a proteção robusta de dados pessoais, ao mesmo tempo em que permitiria aos titulares de dados tomar medidas para sua própria proteção caso seus dados sejam comprometidos.

No entanto, qualquer proposta deve ser elaborada cuidadosamente para evitar notificações irrelevantes, principalmente assegurando que a notificação seja exigida somente quando exista risco grave de dano ao usuário. Além disso, devem ser excluídos da obrigação de notificação todos os casos em que os dados comprometidos em questão tenham sido considerados inutilizáveis, ilegíveis ou indecifráveis por um terceiro não-autorizado devido ao uso de práticas ou métodos amplamente aceitos como práticas ou padrões vigentes do setor.

Se for exigida uma notificação de violação, esta deve ocorrer num prazo razoável, tendo em conta o tempo necessário para avaliar a natureza e o âmbito da violação e se a violação é susceptível de causar danos significativos ao titular dos dados.

Modificações recomendadas

Art. 47 O responsável deverá comunicar ao órgão competente a ocorrência de ~~qualquer~~ incidentes de segurança graves que possam acarretar danos ~~risco ou prejuízo~~ ~~relevante~~ significativos aos titulares.

Parágrafo único. A comunicação será feita em prazo razoável, conforme definido pelo órgão competente, levando em conta o tempo necessário para avaliar a natureza e o escopo do incidente e se há a possibilidade de o incidente causar dano significativo ao titular, e deverá mencionar, no mínimo:

I – a descrição da natureza dos dados pessoais afetados;

II – as informações sobre os titulares envolvidos;

III – a indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de enriptação;

IV – os riscos relacionaos ao incidente;

V – os motivos da demora, no caso da comunicação não ter sido imediata; e

VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

INÍCIO DA VIGÊNCIA DA LEI (*VACATIO LEGIS*)

Devido à complexidade das obrigações estabelecidas pela nova legislação, recomendamos que seja concedido um prazo de pelo menos 2 (dois) anos para permitir a adaptação das empresas às novas regras.

Modificações recomendadas

Art. 56. Esta Lei entra em vigor dois anos ~~cento e oitenta dias~~ após a data da sua publicação.

Parágrafo único. O órgão competente estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento e a natureza dos dados.

Mais uma vez, gostaríamos de agradecer a oportunidade de poder oferecer essas sugestões e esperamos que as mesmas contribuam para a criação

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

de políticas públicas que permitam mais inovação e crescimento econômico gerado pela economia digital no Brasil

Esperamos continuar participando desta importante discussão e colocamo-nos à disposição para esclarecer quaisquer dúvidas.

Respeitosamente,

Leticia S. Lewis
Diretora, Políticas Públicas
BSA|The Software Alliance